EXHIBIT 6

PRELIMINARY CLAIM CHART

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
A method, comprising: at at least one server: identifying first vulnerability information utilizing second vulnerability information that is used to identify a plurality of potential vulnerabilities, the first vulnerability information being identified by:	Trend Micro Apex Central, when in operation, practices *a method, comprising: at at least one server* (e.g., one or more servers that includes, accesses, and/or serves Trend Micro Apex Central, etc.)*: identifying first vulnerability information* (e.g., a smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, including associated information, including but not limited to information describing the actual vulnerabilities themselves, information describing endpoints that contain the particular operating system/application/version thereof, information describing policy/detection/remediation techniques for addressing the actual vulnerabilities relevant to the particular operating system/application/version thereof including signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *utilizing second vulnerability information* (e.g., a larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof, including associated information, including but not limited to information describing the possible vulnerabilities themselves, information describing the different operating systems/applications/versions thereof, information describing policy/detection/remediation techniques for addressing the potential vulnerabilities relevant to the different operating systems/applications/versions thereof including signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *that is used to identify a plurality of potential vulnerabilities* (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.)*, the first vulnerability information being identified by:* **Note**: See, for example, the evidence below (emphasis added, if any):

EXHIBIT 6

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

	"**About the Web Console** The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console lets you administer the Apex Central network from any machine using a compatible web browser. Apex Central supports the following web browsers: • Microsoft Internet Explorer™ 11 • Microsoft Edge™ • Google Chrome™ **Web Console Requirements**

Resource	Requirement
Processor	300 MHz Intel™ Pentium™ processor or equivalent
RAM	128 MB minimum
Available disk space	30 MB minimum
Browser	Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™ Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.

Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 2-2 to 2-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>“Attack Discovery Detection Information

<u>Provides general information about threats detected by Attack Discovery</u>

<table>
<tr><th>Data</th><th>Description</th></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Endpoint</td><td>The name of the endpoint</td></tr>
<tr><td>Product</td><td>The name of the managed product or service</td></tr>
<tr><td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr>
<tr><td>Product Version</td><td>The version of the managed product</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr>
<tr><td>Pattern Version</td><td>The Attack Discovery pattern number for the detection type</td></tr>
<tr><td>Rule ID</td><td>The serial number of the detection rule</td></tr>
<tr><td>Rule Name</td><td>The rules which specify behaviors to be detected by Attack Discovery</td></tr>
<tr><td>Related Objects</td><td>The number of detections

Click the count to view additional details.

For more information, see Detailed Attack Discovery Detection Information on page B-11.</td></tr>
</table></td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Generated (Local Time)</td><td>The time in the agent's local timezone when Attack Discovery detected the threat

The time is displayed with the UTC offset.</td></tr>
<tr><td>Instance ID</td><td>The detection ID assigned to the event

Entries having the same instance ID belong under the same event.</td></tr>
<tr><td>Tactics</td><td>The MITRE ATT&CK™ tactic(s) detected

For more information, see https://attack.mitre.org/tactics/enterprise/.</td></tr>
<tr><td>Techniques</td><td>The MITRE ATT&CK™ technique(s) detected

For more information, see https://attack.mitre.org/techniques/enterprise/.</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about: • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 25-2 to 25-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
identifying at least one operating system of a plurality of devices, and	Trend Micro Apex Central, when in operation, practices a method for *identifying at least one operating system* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) *of a plurality of devices* (e.g., managed products and endpoints, etc.)*, and* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Vulnerability attack** Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems (pg 3-10)" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 3-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "Procedure

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	1. Go to **Administration > Security Agent Download**. 2. Select the operating system. • **Windows 64-bit**: Select to create a 64-bit MSI installation package for Apex One Security Agents • **Windows 32-bit**: Select to create a 32-bit MSI installation package for Apex One Security Agents • **Mac OS**: Select to create a ZIP installation package for Apex One (Mac) Security Agents" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 9-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "**About Apex Central** Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 1-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>based on the at least one operating system, identifying at least one of the plurality of potential vulnerabilities as an actual vulnerability of a plurality of actual vulnerabilities of the at least one operating system to which the plurality of devices is actually vulnerable; and</td><td>Trend Micro Apex Central, when in operation, practices a method for, based on the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.), identifying at least one of the plurality of potential vulnerabilities (e.g., the possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.) as an actual vulnerability of a plurality of actual vulnerabilities (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) of the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) to which the plurality of devices (e.g., managed products and endpoints, etc.) is actually vulnerable; and

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

“The Threat Type column displays the following threat types.

<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td>Known Advanced Persistent Threat (APT)</td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>communicating, from the at least one server and to at least one of the plurality of devices over at least one network, the first vulnerability information, the first vulnerability information corresponding with the actual vulnerabilities of the at least one operating system of the at least one device, and excluding at least a portion of the second vulnerability</td><td>Trend Micro Apex Central, when in operation, practices a method for communicating, from the at least one server (e.g., the one or more servers that includes, accesses, and/or serves Trend Micro Apex Central, etc.) and to at least one of the plurality of devices (e.g., one of the managed products and endpoints, etc.) over at least one network, the first vulnerability information (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof), the first vulnerability information corresponding with the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) of the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) of the at least one device (e.g., one of the managed products and endpoints, etc.), and excluding at least a portion of the second vulnerability information (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof)</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	*that does not correspond with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) *of the at least one device* (e.g., one of the managed products and endpoints, etc.); **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: As set forth below, Trend Micro Apex Central includes software that generates (and communicates to the managed products and endpoints) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software available at the Trend Micro ActiveUpdate server and/or other update servers). As set forth below, once configured, the Trend Micro ActiveUpdate server and/or other servers automatically determine which of the updates to generate and communicate. "**Component Updates** The Apex Central server hosts component files that the managed products use to keep your network protected from the latest security threats. Keep the components up-to-date by running manual or scheduled updates. Apex Central allows you to perform the following tasks:

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>

Download the latest component versions from an update source
Deploy updated components to managed products

“Update Source

Configure the Apex Central server to download components from the Trend Micro ActiveUpdate server or other update sources. You can specify other update sources if the Apex Central server is unable to connect to the Trend Micro ActiveUpdate server directly or if you host an update server in your network.

By default, Apex Central uses a more secure HTTPS connection method to download components from the Trend Micro ActiveUpdate server.

To access other update sources, Apex Central supports Remote UNC authentication, which uses a user account from the update source server to share a folder for Apex Central to download updates.”
Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 11-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View

<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<table><tr><td></td><td>endpoints with ***recommended Intrusion Prevention*** rules based on your network performance and security priorities.</td></tr><tr><td>…</td><td>…</td></tr></table> https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx "**Intrusion Prevention Rules** The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection. • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "… 5. In the Certified Safe Software List section, configure the following:

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	• **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)
at the at least one device: receiving, from the at least one server over the at least one	Trend Micro Apex Central, when in operation, practices a method for, *at the at least one device* (e.g., one of the managed products and endpoints, etc.)*: receiving, from the at least one server* (e.g., the one or more servers that includes, accesses, and/or serves Trend Micro Apex Central,

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>network, the first vulnerability information;</td><td>etc.) over the at least one network, the first vulnerability information (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

<u>Note</u>: As set forth below, Trend Micro Apex Central includes software that generates (and communicates to the managed products and endpoints) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software available at the Trend Micro ActiveUpdate server and/or other update servers). As set forth below, once configured, the Trend Micro ActiveUpdate server and/or other servers automatically determine which of the updates to generate and communicate.

<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td><u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans</u>. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 10-13 (<u>https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</u>)</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View

<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with recommended Intrusion Prevention rules based on your network performance and security priorities.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx "**Intrusion Prevention Rules** The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection. • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "... 5. In the Certified Safe Software List section, configure the following: • **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	• **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)
identifying a first portion of the first vulnerability information that includes data inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of	Trend Micro Apex Central, when in operation, practices a method for *identifying a first portion of the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof) *that includes data inspection-related information* (e.g., antivirus pattern information or the data loss prevention information, etc.) *that corresponds with at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>the at least one device, and that excludes other data inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;</td><td>application/version thereof, etc.) of the at least one device (e.g., one of the managed products and endpoints, etc.), and that excludes other data inspection-related information of the second vulnerability information (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) that does not correspond with the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) of the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) of the at least one device (e.g., one of the managed products and endpoints, etc.);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td><u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans</u>. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>…

Table 1. Product Status Information Data View

<table><tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr><tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr><tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr></table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

“Compliance Indicators

 

This section of the Operation Center tab provides information about the antivirus pattern information or the data loss prevention information level of your network.

As your network compliance level changes, the color of the compliance indicator icon changes to reflect the thresholds configured on the Active Directory and Compliance Settings screen.

The default view displays information for the Antivirus pattern compliance indicator.”</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-7 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

<table><tr><th>Update Method</th><th>Description</th></tr><tr><td>Antivirus pattern compliance</td><td>Displays the following information:

• The percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions
• The total number of endpoints with outdated antivirus patterns on your network

Click the count for Endpoints with outdated patterns to view detailed information about the affected endpoints in the User/Endpoint Directory.</td></tr></table>Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 1-7 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf)</td></tr>
<tr><td>identifying a first event of a plurality of events in connection with the at least one device;

causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is susceptible to</td><td>Trend Micro Apex Central, when in operation, practices a method for identifying a first event of a plurality of events (e.g., a first discrete event that triggers at least one of the signature/policy updates for the anti-virus/data loss prevention software, etc.) in connection with the at least one device (e.g., one of the managed products and endpoints, etc.); causing a determination that the at least one of the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) corresponding with the data inspection-related information (e.g., antivirus pattern information or the data loss prevention information, etc.) is susceptible to being taken advantage of by the first event (e.g., the first discrete event that triggers at least one of the signature/policy updates for the anti-virus/data</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>being taken advantage of by the first event identified in connection with the at least one device, utilizing the data inspection-related information;

identifying a second event of the plurality of events in connection with the at least one device;

causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is not susceptible to being taken advantage of by the second event identified in connection with the at least one device, utilizing the data inspection-related information;</td><td>loss prevention software, etc.) identified in connection with the at least one device (e.g., one of the managed products and endpoints, etc.), utilizing the data inspection-related information (e.g., antivirus pattern information or the data loss prevention information, etc.); identifying a second event of the plurality of events (e.g., a second discrete event that does <u>not</u> trigger any of the signature/policy updates for the anti-virus/data loss prevention software, etc.) in connection with the at least one device (e.g., one of the managed products and endpoints, etc.); causing a determination that the at least one of the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) corresponding with the data inspection-related information (e.g., antivirus pattern information or the data loss prevention information, etc.) is not susceptible to being taken advantage of by the second event (e.g., the second discrete event that does <u>not</u> trigger any of the signature/policy updates for the anti-virus/data loss prevention software, etc.) identified in connection with the at least one device (e.g., one of the managed products and endpoints, etc.), utilizing the data inspection-related information (e.g., antivirus pattern information or the data loss prevention information, etc.);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

<u>Note</u>: Antivirus pattern compliance includes signatures/policies that are triggered by some events (e.g., the first event, etc.), and that are not triggered by other events (e.g., the second event, etc.), so that only malicious events (relevant to the device’s operating system) trigger a response.

<table>
<tr><th>Indicator</th><th>Description</th></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th colspan="2">Applicability</th></tr>
<tr><td></td><td>Antivirus pattern compliance</td><td>Displays the percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions

You can also view the following details:

• Managed agents: The number of endpoints that have Security Agents installed
o With compliant virus patterns: The number of managed agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions
o With outdated virus patterns: The number of managed agents not using acceptable Virus Pattern and Smart Scan Agent Pattern versions
o Offline for 7 days: The number of managed agents that have not communicated with the managed product server in 7 or more days
o Exceptions: The number of users or endpoints excluded from the compliance calculations
• Unmanaged endpoints: The number of endpoints that do not have Security Agents installed

Expand the categories and click a count to view additional details about the affected endpoints.
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>identifying a second portion of the first vulnerability information that includes traffic inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other traffic inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;</td><td>Trend Micro Apex Central, when in operation, practices a method for identifying a second portion of the first vulnerability information (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) that includes traffic inspection-related information (e.g., intrusion detection rules, etc.) that corresponds with at least one of the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) of the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) of the at least one device (e.g., one of the managed products and endpoints, etc.), and that excludes other traffic inspection-related information (e.g., threat discovery, etc.) of the second vulnerability information (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) that does not correspond with the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) of the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) of the at least one device (e.g., one of the managed products and endpoints, etc.);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td><u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans</u>. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View

<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>endpoints with <u>recommended Intrusion Prevention</u> rules based on your network performance and security priorities.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

“Intrusion Prevention Rules

The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.”
Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

“…
5. In the Certified Safe Software List section, configure the following:</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>

Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.

Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.

<u>Important</u>: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.”
https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)

“The Threat Type column displays the following threat types.

<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td><u>Known Advanced Persistent Threat (APT)</u></td><td><u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u></td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>identifying a third event of the plurality of events in connection with the at least one device;

causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is susceptible to being taken advantage of by the third event identified in connection with the</td><td>Trend Micro Apex Central, when in operation, practices a method for identifying a third event of the plurality of events (e.g., a third event that triggers at least one of the signature/policy updates for the intrusion prevention rules, etc.) in connection with the at least one device (e.g., one of the managed products and endpoints, etc.); causing a determination that the at least one of the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) corresponding with the traffic inspection-related information (e.g., intrusion detection rules, etc.) is susceptible to being taken advantage of by the third event (e.g., the third event that triggers at least one of the signature/policy updates for the intrusion prevention rules, etc.) identified in connection with the at least one device (e.g., one of the managed products and endpoints, etc.), utilizing the traffic inspection-related information (e.g., intrusion detection rules, etc.); identifying a fourth event of the plurality of events (e.g., a fourth event that does not trigger at least one of the signature/policy updates for the intrusion</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
at least one device, utilizing the traffic inspection-related information; identifying a fourth event of the plurality of events in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is not susceptible to being taken advantage of by the fourth event identified in connection with the at least one device, utilizing the traffic inspection-related information;	prevention rules, etc.) *in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the traffic inspection-related information* (e.g., intrusion detection rules, etc.) *is not susceptible to being taken advantage of by the fourth event* (e.g., the fourth event that does not trigger at least one of the signature/policy updates for the intrusion prevention rules, etc.) *identified in connection with the at least one device* (e.g., one of the managed products and endpoints, etc.)*, utilizing the traffic inspection-related information* (e.g., intrusion detection rules, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: The intrusion prevention rules include signatures/policies that are triggered by some events (e.g., the third event, etc.), and that are not triggered by other events (e.g., the fourth event, etc.), so that only malicious events (relevant to the device's operating system) trigger a response. "**Intrusion Prevention Rules** The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	• To filter the list of rules, use the **Search** box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
identifying a third portion of the first vulnerability information that includes firewall-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other firewall-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	Trend Micro Apex Central, when in operation, practices a method for *identifying a third portion of the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof) *that includes firewall-related information* (e.g., firewall configuration information, etc.) *that corresponds with at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) *of the at least one device* (e.g., one of the managed products and endpoints, etc.), *and that excludes other firewall-related information of the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that does not correspond with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) *of the at least one device* (e.g., one of the managed products and endpoints, etc.); **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View
<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<table><tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr></table> Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center "... 5. In the Certified Safe Software List section, configure the following: • **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**."

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)

“Detailed Firewall Violation Information

Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”

<table>
<tr><th>Section</th><th>Settings</th></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Product Entity/Endpoint</td><td>Depending on the related source:

• The display name of the managed product server in Apex Central
• The name or IP address of the endpoint Product</td></tr>
<tr><td>Product</td><td>The name of the managed product or service

Example: Apex One, ScanMail for Microsoft Exchange</td></tr>
<tr><td>Event Type</td><td>The type of event that triggered the detection

Example: intrusion, policy violation</td></tr>
<tr><td>Risk Level</td><td>The Trend Micro assessment of risk to your network</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Example: High security, low security, medium security</td></tr>
<tr><td>Traffic/Connection</td><td>The direction of the transmission</td></tr>
<tr><td>Protocol</td><td>The protocol the intrusion uses

Example: HTTP, SMTP, FTP</td></tr>
<tr><td>Source IP</td><td>The source IP address of the detected threat</td></tr>
<tr><td>Endpoint Port</td><td>The port number of the endpoint under attack</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Target Application</td><td>The application the intrusion targeted</td></tr>
<tr><td>Description</td><td>The detailed description of the incident by Trend Micro</td></tr>
<tr><td>Action</td><td>The action taken by the managed product

Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections

Example: A managed product detects 10 violation instances of the same type on one computer

Detections = 10</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</td></tr>
<tr><td>identifying a fifth event of the plurality of events in connection with the at least one device;</td><td>Trend Micro Apex Central, when in operation, practices a method for identifying a fifth event of the plurality of events (e.g., a fifth event that triggers at least one of the signature/policy updates for the firewall violation software, etc.) in connection with the at least one device (e.g., one of the managed products and endpoints, etc.); causing a determination that the at least one of the</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
causing a determination that the at least one of the actual vulnerabilities corresponding with the firewall-related information is susceptible to being taken advantage of by the fifth event identified in connection with the at least one device, utilizing the firewall-related information; identifying a sixth event of the plurality of events in connection with the at least one device; and causing a determination that the at least one of the actual vulnerabilities corresponding with the firewall-related information is not susceptible to being taken advantage of by the sixth event identified in connection with the at least one device, utilizing the firewall-related information; and	*actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the firewall-related information* (e.g., firewall configuration information, etc.) *is susceptible to being taken advantage of by the fifth event* (e.g., the fifth event that triggers at least one of the signature/policy updates for the firewall violation software, etc.) *identified in connection with the at least one device* (e.g., one of the managed products and endpoints, etc.)*, utilizing the firewall-related information* (e.g., firewall configuration information, etc.)*; identifying a sixth event of the plurality of events* (e.g., a sixth event that does not trigger at least one of the signature/policy updates for the firewall violation software, etc.) *in connection with the at least one device* (e.g., one of the managed products and endpoints, etc.)*; and causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the firewall-related information* (e.g., firewall configuration information, etc.) *is not susceptible to being taken advantage of by the sixth event* (e.g., the sixth event that does not trigger at least one of the signature/policy updates for the firewall violation software, etc.) *identified in connection with the at least one device* (e.g., one of the managed products and endpoints, etc.)*, utilizing the firewall-related information* (e.g., firewall configuration information, etc.)*; and* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "… 5. In the Certified Safe Software List section, configure the following: • **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	• **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added) "**Detailed Firewall Violation Information** Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations" **Section** | **Settings**

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability	
	Received	The date and time Apex Central received the data from the managed product
	Generated	The date and time the managed product generated the data
	Product Entity/Endpoint	Depending on the related source: • The display name of the managed product server in Apex Central • The name or IP address of the endpoint Product
	Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange
	Event Type	The type of event that triggered the detection Example: intrusion, policy violation
	Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security
	Traffic/Connection	The direction of the transmission
	Protocol	The protocol the intrusion uses Example: HTTP, SMTP, FTP
	Source IP	The source IP address of the detected threat
	Endpoint Port	The port number of the endpoint under attack
	Endpoint IP	The IP address of the endpoint
	Target Application	The application the intrusion targeted
	Description	The detailed description of the incident by Trend Micro

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Action</td><td>The action taken by the managed product

Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections

Example: A managed product detects 10 violation instances of the same type on one computer

Detections = 10</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>at at least one administrator computer:

in response to administrator action, causing setting, before the first and second events, of a first policy associated with utilizing the data inspection-related information that is applied to a group including each of the plurality of devices that has the at least one operating system;</td><td>Trend Micro Apex Central, when in operation, practices a method for, at at least one administrator computer (e.g., any machine with a web console that lets you administer the Apex Central network, etc.): in response to administrator action (e.g., user input, etc.), causing setting, before the first and second events, of a first policy (e.g., a security policy designed for use in enforcing antivirus pattern compliance or data loss prevention compliance, etc.) associated with utilizing the data inspection-related information (e.g., antivirus pattern information or the data loss prevention information, etc.) that is applied to a group including each of the plurality of devices (e.g., managed products and endpoints, etc.) that has the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</td></tr>
</table>

"**About the Web Console**

The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console lets you administer the Apex Central network from any machine using a compatible web browser.

Apex Central supports the following web browsers:

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- Google Chrome™

Web Console Requirements

Resource	Requirement
Processor	300 MHz Intel™ Pentium™ processor or equivalent
RAM	128 MB minimum
Available disk space	30 MB minimum
Browser	Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™ Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.

Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 2-2 to 2-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<u>Note</u>: As set forth below, a security policy is capable of being set for use in enforcing antivirus pattern compliance or data loss prevention compliance.

“Each managed product provides different policy settings that you can <u>configure</u> and deploy to policy targets.”
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx
(emphasis added)

“Configuring the Antivirus Pattern Compliance Indicators

You can configure settings and exceptions for the Antivirus Pattern Compliance indicators to display the percentage of managed Security Agents using acceptable antivirus pattern (Virus Pattern and Smart Scan Agent Pattern) versions on the Operation Center tab.

1. Go to Administration > Settings > Active Directory and Compliance Settings.
2. Click the Compliance Indicator tab.
3. Click Antivirus pattern compliance.

The following table describes the available configuration options.

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Acceptable pattern versions</td><td>Specify the pattern versions for endpoints to be considered compliant.</td></tr>
<tr><td>Alert indicator</td><td>Adjust the slider control to set the thresholds (% of compliant agents) for different alert levels.</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	4. In the **Exception List**, select custom tags or filters to exclude users or endpoints from compliance calculations. **Note**: The Exceptions list applies to all Apex Central users. You may only add or delete exceptions based on your permissions to modify the corresponding tags and filters. For more information about creating tags or filters, see Custom Tags and Filters. a. Click **Add**. The Add Exception screen appears. b. From the **Type** drop-down list, select **User** or **Endpoint** to display the available custom filters and tags by type; otherwise, select All to view all entries. **Note**: To search for a custom filter or tag, type a name in the text field and press ENTER. For more information on custom tags and filters, see Custom Tags and Filters. c. Select one or more custom tags or filters and click **Add**. The selected items appear in the Exception List. d. Click **Close**. e. Click **Save**.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	f. Specify the scope of the added custom tags or filters from the **Apply exceptions added by** drop-down list. **All user accounts**: Excludes all users and endpoints specified in custom filters and tags added by any user account **Only the logged on account**: Excludes only the users and endpoints specified in custom filters and tags added by the currently logged on user account 5. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/getting-started/active-directory-and_001/compliance-indicator_001/configuring-the-anti.aspx "**Data Loss Prevention** Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data-referred to as digital assets-against accidental disclosure and intentional theft. DLP allows you to: • Identify the digital assets to protect • Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices • Enforce compliance to established privacy standards

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 14-14 to 14-15 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
in response to administrator action, causing setting, before the third and fourth events, of a second policy associated with utilizing the traffic inspection-related information that is applied the group including each of the plurality of devices that has the at least one operating system; and	Trend Micro Apex Central, when in operation, practices a method for, *in response to administrator action* (e.g., user input, etc.)*, causing setting, before the third and fourth events, of a second policy* (e.g., a security policy designed for use in enforcing intrusion detection rule compliance, etc.) *associated with utilizing the traffic inspection-related information* (e.g., intrusion detection rules, etc.) *that is applied the group including each of the plurality of devices* (e.g., managed products and endpoints, etc.) *that has the at least one operating system* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.)*; and* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: As set forth below, a security policy is capable of being set for use in enforcing intrusion detection rule compliance. "Each managed product provides ***different policy settings*** that you can ***configure*** and deploy to policy targets." https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx (emphasis added)

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	"**Intrusion Prevention Rules** The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection. • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "**Endpoint Sensor** Endpoint Sensor is a powerful monitoring and investigation tool used to identify the presence, location, and entry point of threats. Through the use of detailed system event recording and historical analysis, you can perform preliminary investigations to discover hidden threats throughout your network and locate all affected endpoints. Generate root cause analysis reports to understand the nature and activity of the malware since the threat entered the endpoint.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	You can also perform detailed investigations through the use of shared IOC files and YARA rules. Detailed investigations conduct in-depth, live searches of endpoints to locate previously unidentified threats and possible Advanced Persistent Threat attacks. **Configuring Endpoint Sensor Settings** **Important**: The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider. **Procedure** 1. Select **Enable Endpoint Sensor**. 2. Select **Enable event recording** to begin collecting system event logs on the agent endpoint. Endpoint Sensor uses the real-time event logs to identify at-risk endpoints when performing investigations. After identifying affected Windows endpoints, you can perform an in-depth root cause analysis to better understand possible attack vectors." *Trend Micro Apex Central Widget and Policy Management Guide*, Version: 2019, Page 14-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf) "**Creating a New Policy**

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Important: Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*. 1. Go to **Policies > Policy Management**. The Policy Management screen appears. 2. Select the type of product settings from the **Product** list. The screen refreshes to display policies created for the selected managed product. For more information about configuring policy settings for specific managed products, see the *Apex Central Widget and Policy Management Guide*. 3. Click **Create**. The Create Policy screen appears. 4. Type a policy name. 5. Specify targets. Apex Central provides several target selection methods that affect how a policy works. The policy list arranges the policy targets in the following order: • **Specify Targets**: Use this option to select specific endpoints or managed products. For details, see Specifying Policy Targets. • **Filter by Criteria**: Use this option to allocate endpoints automatically based on the filtering criteria. For details, see Filtering by Criteria.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	• **None (Draft only)**: Use this option to save the policy as a draft without choosing any targets. For more information about the policy list, see Understanding the Policy List. 6. Click a managed product feature to expand it and configure its settings. Repeat this step to configure all features. • Each feature has a link to a Help topic that discusses the feature and how to use it. • For certain product settings, Apex Central needs to obtain specific setting options from the managed products. If administrators select multiple targets for a policy, Apex Central can only obtain the setting options from the first selected target. To ensure a successful policy deployment, make sure the product settings are synchronized across the targets. • If you are creating a policy for **Apex One Security Agent** that you want to act as a parent to a future child policy, configure settings that can be inherited, customized, or extended on the child policy. • For a list of Security Agent settings that can be inherited, customized, or extended, see Working with Parent Policy Settings. • For details on creating a child policy, see Inheriting Policy Settings.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	7. Click **Deploy** or **Save**. If you clicked Deploy, Apex Central starts the deployment. The deployed policy appears in the list on the Policy Management screen. It usually takes a few minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the Policy Management screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Apex Central and the targets. Also check if the targets are working properly. Once Apex Central deploys a policy to the targets, the settings defined in the policy overwrite the existing settings in the targets. Apex Central enforces the policy settings in the targets every 24 hours. Although local administrators can make changes to the settings from the managed product console, the changes are overwritten every time Apex Central enforces the policy settings. • Apex Central enforces the policy settings on the targets every 24 hours. Since policy enforcement only occurs every 24 hours, the product settings in the targets may not align with the policy settings if local administrators make changes through the managed product console between the enforcement period. • Policy settings deployed to IMSVA servers take priority over the existing settings on the target servers instead of overwriting them. IMSVA servers save these policy settings on the top of the list. • If an Apex One Security Agent assigned with a Apex Central policy has been moved to another Apex One domain, the agent settings will temporarily change to the ones defined

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	by that Apex One domain. Once Apex Central enforces the policy again, the agent settings will comply with the policy settings." https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx
in response to administrator action, causing setting, before the fifth and sixth events, of a third policy associated with utilizing the firewall-related information that is applied to the group including each of the plurality of devices that has the at least one operating system.	Trend Micro Apex Central, when in operation, practices a method for, *in response to administrator action* (e.g., user input, etc.)*, causing setting, before the fifth and sixth events, of a third policy* (e.g., a security policy designed for use in enforcing prevent firewall compliance, etc.) *associated with utilizing the firewall-related information* (e.g., firewall configuration information, etc.) *that is applied to the group including each of the plurality of devices* (e.g., managed products and endpoints, etc.) *that has the at least one operating system* (e.g.*,* Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.). **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: As set forth below, a security policy is capable of being set for use in enforcing firewall compliance. "Each managed product provides ***different policy settings*** that you can ***configure*** and deploy to policy targets." https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx (emphasis added) "**Configuring Additional Security Agent Services**

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
Procedure

1. <u>Select to enable the required service on Windows desktops or Windows Server platforms</u> in the following sections:

• Unauthorized Change Prevention Service
o For Windows Server platforms, select Only enable services required by Security Agent Self-protection features to ensure that the Security Agent program stays protected without affecting server performance.
• ...
• <u>Firewall Service</u>

<u>Important</u>: Enabling or disabling the service temporarily disconnects endpoints from the network. Ensure that you change the settings only during non-critical hours to minimize connection disruptions.

• Suspicious Connection Service
• Data Protection Service
...”
Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 6-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf)

<table>
<tr><th>Section</th><th>Settings</th></tr>
</table>
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Firewall</td><td>
• Display the Firewall settings on the Security Agent console: Allows users to configure the Firewall settings on the Security Agent console

• Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message: Displays the Enable/Disable Firewall and Enable/Disable IDS Mode menu options on the Security Agent system tray icon

<u>Note</u>: The Apex One Firewall protects agents and servers on the network using stateful inspection, high performance network virus scanning, and elimination. If you grant users the privilege to enable or disable the firewall and its features, warn them not to disable the firewall for an extended period of time to avoid exposing the endpoint to intrusions and hacker attacks.

• Allow Security Agents to send firewall logs to the Apex One server: Configures the Security Agent to send Firewall logs to the server, allowing you to analyze network traffic
</td></tr>
</table>
Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 6-6 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf)

“Adding a Firewall Policy
</td></tr>
</table>

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	1. Go to **Agents > Firewall > Policies**. 2. Select to add, copy, or modify a policy. • Click Add to create a new policy. • Select an existing policy and click **Copy** to open the **Copy Policy** screen. Modify the policy settings as required. • Click the **Policy Description** of an existing policy to modify settings. 3. In the **Firewall Policy** section, configure the following: • **Name**: Specify a unique name for the Apex One Firewall policy. • **Security level**: Select from High, Medium, or Low to determine the type of traffic that the Apex One Firewall allows or blocks. **Note**: The Apex One Firewall automatically allows or blocks connections through the ports specified in the Exception Template list. For more information, see Editing the Apex One Firewall Exception Template List. 4. In the Firewall Features section, configure the following: • **Enable firewall**: Select to activate the Apex One Firewall for this policy.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	• **Enable Intrusion Detection System (IDS)**: Select to attempt and identify patterns in network patterns that may indicate an attack. For more information, see Intrusion Detection System. • **Display a notification when a Firewall violation is detected**: Select to display a notification on the Security Agent when the Apex One Firewall blocks an outgoing packet. **Important**: If you grant users the permission to configure Apex One Firewall settings using the Security Agent console, you cannot use the Apex One web console to override the settings that the user configures. The information under Settings on the Security Agent console's Firewall tab always reflects the settings configured from the Security Agent console, not from the server web console. 5. In the Certified Safe Software List section, configure the following: • **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. o **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.

Patent No. 10,873,595, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the **Exception** section, manage the Exception Template List that applies to this policy only. The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same in connection with any subsequent correlations.